Mac OS X Server Windows Services Administration

For Version 10.3 or Later

Apple Computer, Inc.
© 2003 Apple Computer, Inc. All rights reserved.

The owner or authorized user of a valid copy of Mac OS X Server software may reproduce this publication for the purpose of learning to use such software. No part of this publication may be reproduced or transmitted for commercial purposes, such as selling copies of this publication or for providing paid for support services.

Every effort has been made to ensure that the information in this manual is accurate. Apple Computer, Inc., is not responsible for printing or clerical errors.

The Apple logo is a trademark of Apple Computer, Inc., registered in the U.S. and other countries. Use of the "keyboard" Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, AppleScript, AppleShare, AppleTalk, ColorSync, FireWire, Keychain, Mac, Macintosh, Power Macintosh, QuickTime, Sherlock, and WebObjects are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. AirPort, Extensions Manager, Finder, iMac, and Power Mac are trademarks of Apple Computer, Inc.

Adobe and PostScript are trademarks of Adobe Systems Incorporated.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Netscape Navigator is a trademark of Netscape Communications Corporation.

034-2356/09-20-03

Contents

Preface 7 **About This Guide**
7 Using This Guide
8 Getting Additional Information

Chapter 1 11 **Overview of Windows Services**
12 Providing a PDC for Domain Login
12 Providing Home Directories and Roaming User Profiles
13 Joining a PDC as a Domain Member
13 Providing File, Print, Browsing, and Name Resolution Services
13 Providing VPN Service
14 Tools for Managing Windows Services
14 Server Admin
14 Workgroup Manager
15 Command-Line Tools

Chapter 2 17 **Setting Up Windows Services**
18 Before You Set Up Windows Services
18 Ensuring the Best Cross-Platform Experience
18 Windows User Password Validation
19 Setting the Server's Role and Identity for Windows Services
20 Setting Up a Server of Standalone Windows Services
21 Setting Up a Server as a Windows Domain Member
22 Setting Up a Server as a Primary Domain Controller
23 Changing Windows Services Access Settings
23 Changing Windows Services Logging Settings
24 Changing Windows Services Advanced Settings
25 Starting Windows Services
25 Configuring a Print Queue for SMB Sharing
25 Supporting Windows Client Computers
26 Setting Up Windows Clients for TCP/IP Networking
26 Connecting for File Service From Windows
27 Connecting to the Server by Name or Address in Windows 95, 98, or ME
27 Connecting to the Server by Name or Address in Windows XP

27 Setting Up Windows Clients for Print Service

Chapter 3 29 **Administering Windows Users, Groups, Computers, and Share Points**
29 Setup Overview
30 Managing Accounts for Windows Users
31 Where Windows User Accounts Are Stored
31 Creating Windows User Accounts in the Primary Domain Controller
32 Creating Windows User Accounts in a Read/Write Directory Domain
33 Editing Windows User Accounts
33 Working With Basic Settings for Users
34 Working With Windows Settings for Users
35 Working With Advanced Settings for Users
35 Providing Secure Authentication for Windows Users
36 Working With Group Settings for Users
36 Setting Up a Home Directory for a Windows User
37 Working With Mail Settings for Users
37 Working With Print Settings for Users
37 Defining a Guest User
38 Deleting a Windows User Account
38 Disabling a Windows User Account
38 Managing Groups for Windows Users
39 Working With Group Folder Settings for Windows Groups
39 Managing Windows Workstations in the Windows Computers Account
39 Adding Computers to the Windows Computers Account
40 Removing Computers From the Windows Computers Account
40 Editing Information About a Computer in the Windows Computers Account
40 Moving a Windows Computer to a Different Computer Account
40 Deleting the Windows Computers Account
41 Managing SMB Share Points
41 Opportunistic Locking (oplocks)
41 Strict Locking
42 Creating an SMB Share Point and Setting Privileges
43 Changing Windows (SMB) Settings for a Share Point
44 Managing Share Points

Chapter 4 45 **Migrating Users From a Windows Server to Mac OS X Server**

Chapter 5 51 **Managing Windows Services**
51 Starting and Stopping Windows Services
51 Starting Windows Services
51 Stopping Windows Services
52 Monitoring Windows Services
52 Viewing Windows Services Status

53 Viewing Windows Services Logs
53 Viewing Windows Services Connections
53 Viewing Windows Services Graphs
53 Disconnecting Windows Users
54 Changing the Server's Windows Identity
54 Changing the Server's Windows Computer Name
55 Changing the Server's Windows Domain
55 Changing the Sever's Windows Workgroup
55 Managing Access to Windows Services
55 Allowing Guest Access for Windows Services
56 Limiting the Number of Connected Windows Clients
56 Managing Windows Services Logging
57 Managing Advanced Windows Services Settings
57 Changing the Windows Code Page
57 Enabling Windows Domain Browsing
58 Registering With a WINS Server

Chapter 6 59 **Solving Problems With Windows Services**
59 Problems With a Primary Domain Controller
59 User Can't Log in to the Windows Domain
59 Windows User Has No Home Directory
60 Windows User's Profile Settings Revert to Defaults
60 Windows User Loses Contents of My Documents Folder
60 Problems With Windows File Service
60 User Can't Authenticate for Windows File Service
60 User Can't See the Windows Server in the Network Neighborhood
61 General Problems With File Services
61 Problems With Windows Print Service
61 Windows Users Can't Print
61 General Problems With Print Services

Glossary 63

Index 67

About This Guide

This guide describes the services that Mac OS X Server can provide to Windows computer users and tells you how to set up your server to provide Windows services.

Here is a summary of each chapter's contents:

- Chapter 1, "Overview of Windows Services," highlights important concepts and introduces the tools you use to manage Windows services.
- Chapter 2, "Setting Up Windows Services," explains how to set up Mac OS X Server as a provider of standalone Windows services, a Windows domain member, or a primary domain controller (PDC). Standalone Windows services include file service, print service, Windows Internet Naming Service (WINS), and Windows domain browsing service.
- Chapter 3, "Administering Windows Users, Groups, Computers, and Share Points," tells you how to set up and manage accounts for Windows users, groups, and computers (workstations).
- Chapter 4, "Migrating Users From a Windows Server to Mac OS X Server," explains how to migrate user and group information from a Windows NT server to a Mac OS X Server.
- Chapter 5, "Managing Windows Services," describes how to start and stop Windows services, monitor them, and manage their settings.
- Chapter 6, "Solving Problems With Windows Services,"helps you deal with common problems that occur with a PDC, Windows file service, and Windows print service.
- The Glossary defines terms you'll encounter as you read this guide.

Using This Guide

The chapters in this guide are arranged in the order that you're likely to need them when setting up Mac OS X Server to provide Windows services.

- Review Chapter 1 to acquaint yourself with the Windows services that Mac OS X Server can provide and with the programs you use to set up and manage these services. Chapter 1 also contains information about the tools for managing Windows services.

- Follow the instructions in Chapter 2 to set up Windows services with default settings.
- Read Chapter 3 when you're ready to set up or manage accounts for Windows users, groups, or computers. This includes setting up home directories and roaming user profiles.
- Read Chapter 4 if you need to migrate user accounts from Windows NT servers to Mac OS X Server.
- Use the instructions in Chapter 5 if you need to monitor Windows services, manage access to them, manage their logs, or change their advanced settings.
- Review Chapter 6 if you encounter problems with Windows services.

Getting Additional Information

Mac OS X Server comes with a suite of guides that explain other services and provide instructions for configuring, managing, and troubleshooting them. Most of these documents are on the server discs in the form of PDF files. All of them are available in PDF format from www.apple.com/server/documentation.

This guide	Tells you how to
Mac OS X Server Getting Started For Version 10.3 or Later	Understand the features of Mac OS X Server version 10.3 and prepare your server.
Mac OS X Server Migration To Version 10.3 or Later	Reuse data and service settings on Mac OS X Server version 10.3 that are currently being used on earlier versions of the server.
Mac OS X Server User Management For Version 10.3 or Later	Create and manage user, group, and computer accounts. Set up managed preferences for Mac OS 9 and Mac OS X clients.
Mac OS X Server File Services Administration For Version 10.3 or Later	Share selected server volumes or folders among server clients using these protocols: AFP, NFS, FTP, and SMB.
Mac OS X Server Print Service Administration For Version 10.3 or Later	Host shared printers and manage their associated queues and print jobs.
Mac OS X Server System Image Administration For Version 10.3 or Later	Create disk images and set up the server so that other Macintosh computers can start up from those images over the network. This guide covers NetBoot and Network Install.
Mac OS X Server Mail Service Administration For Version 10.3 or Later	Set up, configure, and administer mail services on the server.
Mac OS X Server Web Technologies Administration For Version 10.3 or Later	Set up and manage a web server, including WebDAV, WebMail, and web modules.
Mac OS X Server Network Services Administration For Version 10.3 or Later	Set up, configure, and administer DHCP, DNS, IP firewall, NAT, and VPN services on the server.

This guide	Tells you how to
Mac OS X Server Open Directory Administration For Version 10.3 or Later	Manage directory and authentication services.
Mac OS X Server QuickTime Streaming Server Administration For Version 10.3 or Later	Set up and manage QuickTime streaming services.
Mac OS X Server: Java Application Server Administration	Deploy and manage J2EE applications using a JBoss application server on Mac OS X Server.
Mac OS X Server Command-Line Administration For Version 10.3 or Later	Use commands and configuration files to perform server administration tasks in a UNIX command shell.

For more information, consult these resources:

- Read Me documents contain important updates and special information. Look for them on the Mac OS X Server discs.
- Online help, available from the Help menu in all the server applications, provides onscreen instructions for administration tasks as well as late-breaking news and web updates.
- Apple support webpages and the AppleCare Knowledge Base provide answers to common questions and the latest information updates. These are available at the following website:
  www.info.apple.com/
- Apple Training offers courses for technical coordinators and system administrators. For a course catalog, visit the following website:
  train.apple.com/
- Discussion groups and mailing lists put you in touch with other server administrators, who may have already found solutions to problems you encounter. To find discussion groups and mailing lists, visit the following websites:
  discussions.info.apple.com/

  www.lists.apple.com/
- The Samba website has information about the open source software on which the Windows services in Mac OS X Server are based. Visit the Samba website at:
  www.samba.org

Overview of Windows Services

1

Windows services encompass a primary domain controller, SMB file and print services, Windows domain browsing, name resolution, and VPN.

Mac OS X Server can provide a variety of services to users of Microsoft Windows 95, 98, ME (Millennium Edition), XP, NT 4.0, and 2000.

- File service allows Windows clients to connect to the server using Server Message Block (SMB) protocol on a TCP/IP network.
- Print service uses SMB to allow Windows clients to print to PostScript printers on the network.
- Windows Internet Naming Service (WINS) allows Windows clients to perform name/address resolution across multiple subnets.
- Domain browsing allows Windows clients to browse for available servers across subnets.
- Virtual private network (VPN) allows Windows clients to securely connect to Mac OS X Server while away from the local network.
- Primary domain controller (PDC) offers:
  - Login to the PDC from Windows NT 4.x, Windows 2000, and Windows XP workstations
  - Users changing their passwords during login
  - Login using the same user account on Mac OS X and Windows computers
  - Roaming user profiles stored on a Mac OS X Server computer
  - Network home directories located on a Mac OS X Server computer
  - User-level security for Windows 95, 98, and ME clients

By providing these services, Mac OS X Server can replace Windows NT servers in small workgroups. Settings for Windows services are grouped In Workgroup Manager and Server Admin, to make them easy to find. These settings are also designed to be familiar to experienced Windows administrators.

Windows services in Mac OS X Server are based on Samba 3, an open source SMB/CIFS server. For more information about Samba, visit the Samba website:

www.samba.org

Providing a PDC for Domain Login

Setting up your Mac OS X Server as a Windows primary domain controller (PDC) enables domain logins for Windows users on your network. Instead of logging in with a user name and password that are defined locally on each workstation, each user can log in with a user name and password that are defined on the PDC. A PDC gives each Windows user one user name and password for logging in from any Windows workstation on the network.

A user needs only one account on Mac OS X Server to log in to Windows workstations and Mac OS X computers. The same user name and password works for Windows domain login and Mac OS X login.

Users can change their passwords while logging in to the Windows domain.

Before you can set up Mac OS X Server as a PDC, you must set up the server as an Open Directory master. The PDC uses the user and computer information stored in the LDAP directory of the Open Directory master.

You have an opportunity to set up an Open Directory master and a PDC when you use Server Assistant after installing Mac OS X Server. You can also set up an Open Directory master and a PDC after installation by using Server Admin.

Be careful to set up only one Mac OS X Server as a PDC on your network. The network can have multiple Open Directory masters, but only one PDC.

Providing Home Directories and Roaming User Profiles

Setting up your Mac OS X Server as a Windows PDC enables it to host home directories and roaming user profiles for Windows users. Alternatively, another Mac OS X Server can host home directories and roaming user profiles.

Each Windows user who logs in to the PDC has a network home directory. If a user puts files or folders in his or her home directory, the user can access them after logging in to the PDC from any Windows workstation that has joined the PDC. The user also has access to the contents of his or her home directory after logging in to a Mac OS X computer. The user has the same network home directory whether logging in to a Windows computer or a Mac OS X computer.

A user's network home directory is located in a share point on a Mac OS X Server. A setting in the user account specifies the share point for the home directory. You can manage home directories with Workgroup Manager.

With roaming profiles, each user has the same profile when he or she logs in to the domain from any Windows workstation on the network. A roaming profile stores a Windows user's preference settings—screensaver, colors, backgrounds, event sounds, web cookies, and so on—in a share point on a Mac OS X Server. A user's roaming profile is stored by default in a predetermined folder on the PDC.

Joining a PDC as a Domain Member

If you have multiple servers with Mac OS X Server on your network, you can set up one as a PDC and set up others to provide additional Windows services. It is important that only one PDC be present on the network.

You join other servers to the Windows domain of the PDC so they can use the PDC for user authentication. Home directories and environment profiles of Windows users can be located in share points on servers that are members of the Windows domain.

Providing File, Print, Browsing, and Name Resolution Services

Whether you set up a PDC or not, you can set up Mac OS X Server to provide other services to Windows users. Starting Windows services on Mac OS X Server enables it to provide access to share points via the Windows standard protocol for file service, server message block (SMB). Windows services also enable Mac OS X Server to provide SMB access to print queues that have been set up for PostScript printers.

In addition, you can set up Mac OS X Server to provide WINS name resolution for Windows clients or to register with an existing WINS server on the network. Mac OS X Server can also provide network browsing service as a workgroup master browser or a domain master browser for Windows clients.

Providing VPN Service

A Mac OS X Server virtual private network (VPN) can include Windows workstations as well as Mac OS X computers. The workstations connect to the server by a private link of encrypted data, simulating a local connection as if the remote computer were attached to the local area network (LAN).

Mac OS X Server VPN uses Microsoft's Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) for authentication. MS-CHAPv2 is also the standard Windows authentication scheme for VPN.

You can set up VPN service in Mac OS X Server to use the Windows standard protocol for encrypted transport of VPN data, which is point-to-point tunneling protocol (PPTP). You can also set up Mac OS X Server VPN service to use an additional protocol, layer two tunneling protocol, secure Internet protocol (L2TP/IPSec).

See the VPN chapter of the network services administration guide for additional information and setup instructions.

Tools for Managing Windows Services

The Workgroup Manager and Server Admin applications provide a graphical interface for managing Windows services in Mac OS X Server. In addition, you can manage Windows services from the command line by using Terminal.

Server Admin

You use Server Admin to

- Set up Mac OS X Server as a PDC, as a Windows domain member, or for standalone Windows services. For instructions, see Chapter 2.
- Manage Windows file and print services, WINS name resolution, and domain browsing. For instructions, see Chapter 5.
- Monitor Windows services. For instructions, see Chapter 5.

See chapter on server administration in the getting started guide for basic information about using Server Admin.

Server Admin is installed in /Applications/Server/.

Workgroup Manager

You use Workgroup Manager to

- Set up and manage user, group, and computer accounts. For instructions, see Chapter 3 of this guide and the chapters on user, group, and computer accounts in the user management guide.
- Manage share points for file service and for user home directories and roaming user profiles. For instructions, see Chapter 5 of this guide and the chapter on share points in the file services administration guide.
- Access the Inspector, which lets you work with Open Directory entries. For instructions, see the maintenance chapter in the Open Directory administration guide.

See the chapter on server administration in the getting started guide for basic information about using Workgroup Manager.

Workgroup Manager is installed in /Applications/Server/.

Command-Line Tools

A full range of command-line tools is available for administrators who prefer to use command-driven server administration. For remote server management, submit commands in a Secure Shell (SSH) session. You can type commands on Mac OS X servers and computers using the Terminal application, located in /Applications/Utilities/. For instructions, see the command-line administration guide.

Setting Up Windows Services

2

You can set up Mac OS X Server to be a standalone Windows services provider, a Windows domain member, or a primary domain controller.

Mac OS X Server can provide several native services to Windows clients:

- Primary domain controller allows each user to log in to the domain using the same user name and password on any Windows workstation, and provides roaming user profiles and network home directories.
- Domain member server automatically authenticates users for its Windows services, such as file service, by using the domain login provided by the primary domain controller. The member server can also host network home directories and roaming user profiles.
- File service allows Windows clients to access files stored in share points on the server using Server Message Block (SMB) protocol over TCP/IP.
- Print service uses SMB to allow Windows clients to print to PostScript printers on the network.
- Windows Internet Naming Service (WINS) allows clients across multiple subnets to perform name/address resolution.
- Windows domain browsing allows clients to browse for available servers across subnets.

You set up Windows services by configuring four groups of settings:

- **General** Specify the server's role in providing Windows services and the server's identity among clients of its Windows services.
- **Access** Limit the number of clients and control guest access.
- **Logging** Choose how much information is recorded in the service log.
- **Advanced** Configure WINS registration and domain browsing services, choose a code page for clients, and control virtual share points for home directories.

Because the default settings work well if you want to provide only Windows file and print services, you may only need to start Windows services. Nonetheless, you should take a look at the settings and change anything that isn't appropriate for your network.

You will have to change some settings if you want to set up Mac OS X Server as a Windows primary domain controller or as a member of the Windows domain of a Mac OS X Server PDC.

In addition to setting up Windows services and clients, you need to set up accounts for Windows users, groups, and computers (workstations). For information, see Chapter 3, "Administering Windows Users, Groups, Computers, and Share Points."

For information on Mac OS X Server directory and authentication services, including Open Directory master and replicas, see the Open Directory administration guide.

Before You Set Up Windows Services

If you plan to provide Windows services from Mac OS X Server, read the following sections for issues you should keep in mind. You should also check the Microsoft documentation for your version of Windows to find out more about the capabilities of the client software. Although Mac OS X Server does not require any special software or configuration on Windows client computers, you may want to read "Supporting Windows Client Computers" on page 25.

Ensuring the Best Cross-Platform Experience

Mac OS and Windows computers store and maintain files differently. For the best cross-platform experience, you should set up at least one share point to be used only by your Windows users. See "Managing SMB Share Points" on page 41.

In addition, you can improve the user experience by following these guidelines:

- Use comparable versions of application software on both platforms.
- Modify files only with the application they were created in.
- If you have Mac OS 8 and Mac OS 9 clients, limit Windows file names to 31 characters.
- Don't use symbols or characters with accents in the names of shared items.

Windows User Password Validation

Mac OS X Server supports several methods of validating user passwords for Windows services. A user account's password type determines the password validation method.

Open Directory Passwords

If a user's account has a password type of Open Directory, the user's password is validated for Windows services by the Open Directory Password Server. This is the recommended password validation method and is required for Windows domain login from a Windows workstation to a Mac OS X Server PDC. An Open Directory password can also be used to authenticate for Windows file service.

Open Directory password validation can be used with user accounts stored in LDAP directory domains as well as NetInfo directory domains. The directory domain does not store the Open Directory password, just a pointer to the Open Directory Password Server and a password ID. The Open Directory Password Server stores passwords in a private database file readable only by the root user, and the contents are encrypted. The Open Directory Password Server never allows passwords to be read over the network—they can only be set and verified.

Shadow Passwords

If a user's account has a password type of shadow password, the user's password is encrypted and stored in a file on the server. Each user's shadow password is stored in a different file, and these files can be read only by the root user. Only user accounts that are stored in a local directory domain can have a shadow password.

A shadow password can be used to authenticate for Windows file service, but can't be used to log in to the Windows domain of a PDC.

Authentication Manager Password

Mac OS X Server supports user accounts that were configured to use the legacy Authentication Manager technology for password validation in Mac OS X Server versions 10.0–10.2. After upgrading a server to Mac OS X Server version 10.3, existing users can continue to use their same passwords. An existing user account uses Authentication Manager if the account is in a NetInfo domain for which Authentication Manager has been enabled and the account is set to use a crypt password.

If you migrate a directory domain from NetInfo to LDAP, all user accounts that used Authentication Manager for password validation are converted to have a password type of Open Directory.

Setting the Server's Role and Identity for Windows Services

You can set up Mac OS X Server to assume any of three roles in providing Windows services:

- **Primary domain controller (PDC)** The server provides Windows file and print services. It also hosts a Windows domain, storing user, group, and computer accounts and providing authentication services to the domain. The PDC server can host user profiles and home directories for users who have user accounts on the PDC.
- **Domain member** The server provides Windows file and print services. It gets authentication services from the Mac OS X Server PDC. A domain member can host user profiles and home directories for users who have user accounts on the PDC.

- **Standalone Windows services** The server provides Windows file and print services. The server authenticates users for its Windows file service, but does not provide authentication services for Windows domain login on Windows computers. This is the default role.

Note: Mac OS X Server can host a PDC only if the server is an Open Directory master.

Important: If your network has multiple Mac OS X Server systems, set up only one as a PDC. The others can be domain members or provide standalone Windows services.

Setting Up a Server of Standalone Windows Services

Using Server Admin, you can set up Mac OS X Server to provide standalone Windows services: file, print, browsing, and Windows Internet Name Service (WINS). The server does not provide authentication services for Windows domain login on Windows computers.

To set up standalone Windows services:

1. Open Server Admin and select Windows for a server in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click General (near the top).
3. Choose Standalone Server from the Role pop-up menu, then enter a description, computer name, and workgroup.

   Description: This description appears in the Network Neighborhood window on Windows computers, and it is optional.

   Computer Name: Enter the name you want Windows users to see when they connect to the server. This is the server's NetBIOS name. The name should contain no more than 15 characters, no special characters, and no punctuation. If practical, make the server name match its unqualified DNS host name. For example, if your DNS server has an entry for your server as "server.example.com," give your server the name "server."

   Workgroup: Enter a workgroup name. Windows users see the workgroup name in the Network Neighborhood window. If you have Windows domains on your subnet, use one of them as the workgroup name to make it easier for clients to communicate across subnets. Otherwise, consult your Windows network administrator for the correct name. The workgroup name cannot exceed 15 characters.
4. Click Save.

For information on configuring individual Windows services, see "Changing Windows Services Access Settings" on page 23, "Changing Windows Services Logging Settings" on page 23, "Changing Windows Services Advanced Settings" on page 24, and the print service administration guide.

From the Command Line

You can also set a server's role in providing Windows services by using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Setting Up a Server as a Windows Domain Member

Using Server Admin, you can set up Mac OS X Server to join a Windows domain hosted by a Mac OS X Server primary domain controller (PDC). A server that joins a Windows domain gets authentication services from the PDC. This domain member server can also provide file, print, browsing, and Windows Internet Name Service (WINS). The server can host user profiles and home directories for users who have user accounts on the PDC. The domain member server does not provide authentication services to other domain members.

To join Mac OS X Server to the Windows domain of a Mac OS X Server PDC:

1. Open Server Admin and select Windows for a server in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click General (near the top).
3. Choose Domain Member from the Role pop-up menu, then enter a description, computer name, and domain.

   Description: This description appears in the Network Neighborhood window on Windows computers, and it is optional.

   Computer Name: Enter the name you want Windows users to see when they connect to the server. This is the server's NetBIOS name. The name should contain no more than 15 characters, no special characters, and no punctuation. If practical, make the server name match its unqualified DNS host name. For example, if your DNS server has an entry for your server as "server.example.com," give your server the name "server."

   Domain: Enter the name of the Windows domain that the server will join. The domain must be hosted by a Mac OS X Server PDC. The name cannot exceed 15 characters and cannot be "WORKGROUP."
4. Click Save.
5. Enter the name and password of a user account that can administer the LDAP directory domain on the PDC server, then click OK.

For information on configuring individual Windows services, see "Changing Windows Services Access Settings" on page 23, "Changing Windows Services Logging Settings" on page 23, "Changing Windows Services Advanced Settings" on page 24, and the print service administration guide.

From the Command Line

You can also set a server's role in providing Windows services by using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Setting Up a Server as a Primary Domain Controller

Using Server Admin, you can set up Mac OS X Server as a Windows primary domain controller (PDC). The PDC hosts a Windows domain and provides authentication services to other domain members, including authentication for domain login on Windows workstations. The PDC server can provide other Windows services: file, print, browsing, and Windows Internet Name Service (WINS). The server can host user profiles and home directories for users who have user accounts on the PDC.

To set up a Windows PDC:

1. Make sure the server is an Open Directory master.

   To determine whether a server is an Open Directory master, open Server Admin, select Open Directory for the server in the Computers & Services list, click Settings (near the bottom of the window), then click General (near the top). If the Role setting is not Open Directory Master, you cannot set up this server to host a PDC. Consult the Open Directory administration guide to learn more about an Open Directory master.

2. In Server Admin's Computers & Services list, select Windows for a server that is an Open Directory master.

3. Click Settings (near the bottom of the window), then click General (near the top).

4. Choose Primary Domain Controller (PDC) from the Role pop-up menu, then enter a description, computer name, and domain.

   Description: This description appears in the Network Neighborhood window on Windows computers, and it is optional.

   Computer Name: Enter the name you want Windows users to see when they connect to the server. This is the server's NetBIOS name. The name should contain no more than 15 characters, no special characters, and no punctuation. If practical, make the server name match its unqualified DNS host name. For example, if your DNS server has an entry for your server as "server.example.com," give your server the name "server."

   Domain: Enter the name of the Windows domain that the server will host. The domain name cannot exceed 15 characters and cannot be "WORKGROUP."

5. Click Save.

6. Enter the name and password of a user account that can administer the LDAP directory domain on the server, then click OK.

For information on configuring individual Windows services, see "Changing Windows Services Access Settings" on page 23, "Changing Windows Services Logging Settings" on page 23, "Changing Windows Services Advanced Settings" on page 24, and the print service administration guide.

From the Command Line

You can also set a server's role in providing Windows services by using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing Windows Services Access Settings

You can use the Access pane of Windows services settings in Server Admin to allow guest users or limit the number of simultaneous client connections.

To configure Windows services Access settings:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click Access (near the top).
3. To allow Windows or other SMB users to connect for Windows file service without providing a user name or password, select "Allow Guest access."
4. To limit the number of users who can be connected for Windows services at one time, select "___ maximum" and type a number in the field.
5. Click Save.

From the Command Line

You can also change the Windows services settings by using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing Windows Services Logging Settings

You can use the Logging pane of Windows services settings in Server Admin to specify how much information is recorded in the Windows log file.

To configure Windows services Logging settings:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Settings (near the bottom of the window), then click Logging (near the top).
3. Choose a level of log detail from the pop-up menu:

   Low records errors and warning messages only.

   Medium records error and warning messages, service start and stop times, authentication failures, and browser name registrations.

   High records error and warning messages, service start and stop times, authentication failures browser name registrations, and all file access.
4. Click Save.

From the Command Line

You can also change Windows services settings using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing Windows Services Advanced Settings

You can use the Advanced pane of Windows services settings in Server Admin to choose a client *code page,* set the server to be a workgroup or domain master browser, specify the server's WINS registration, and enable virtual share points for user homes.

To configure Windows services Advanced settings:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Settings, then click Advanced.
3. Choose the character set you want clients to use from the Code Page pop-up menu.
4. Next to Services, choose whether to enable domain browsing services.

   Workgroup Master Browser provides browsing and discovery of servers in a single subnet.

   Domain Master Browser provides browsing and discovery of servers across subnets.
5. Next to WINS Registration, select how you want the server to register with WINS.

   "Off": prevents your server from using or providing WINS service for browsing outside its local subnet.

   "Enable WINS server": your server provides local name resolution services. This allows clients across multiple subnets to perform name/address resolution.

   "Register with WINS server": your network has a WINS server, and your Windows clients and Windows server are not all on the same subnet. Enter the IP address or DNS name of the WINS server.
6. To simplify setting up share points for Windows user home directories, select "Enable virtual share points."

   If you enable virtual share points, home directories are mounted automatically when Windows users log in to the PDC, and users have the same home directories whether they log in from a Windows workstation or a Mac OS X computer.

   If you disable virtual share points, you have to set up SMB share points for Windows home directories and user profiles, and configure each Windows user account to use these share points.

From the Command Line

You can also change Windows services settings using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Starting Windows Services

You can use Server Admin to start Windows services.

To start Windows services:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Start Service.

From the Command Line

You can also start Windows services using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Configuring a Print Queue for SMB Sharing

You can configure any print queue that has been set up on the server to be shared using SMB. You configure queues for shared printers on the server by using Server Admin.

To create a shared print queue:

1. In Server Admin, select Print in the Computers & Services list.
2. Click Settings, then click Queues.
3. Select the print queue in the list, then click the Edit button (below the list).

   If you don't see the Queues button, you might already be looking at queue settings. Click the Back button (the left-pointing arrow in the upper right).
4. Make sure Sharing Name is compatible with SMB sharing.

   This does not change the Printer Setup Utility queue name on the server.

   Names of queues shared via SMB should be 15 characters maximum and should not contain characters other than A–Z, a–z, 0–9, and _ (underscore).
5. Select the SMB protocol.
6. Click Save, then click the Back button (in the upper right).

Make sure you start Windows services.

Supporting Windows Client Computers

Mac OS X Server supports the native Windows file sharing protocol, Server Message Block (SMB). SMB is also known as Common Internet File System (CIFS). Mac OS X Server comes with built-in browsing and name resolution services for your Windows client computers. You can enable Windows Internet Naming Service (WINS) on your server, or you can register with an existing WINS server.

Windows services in Mac OS X Server include Windows Master Browser and Domain Master Browser services. You do not need a Windows server or a primary domain controller on your network to allow Windows users to see your server listed in the My Places window (Windows XP and 2000) or the Network Neighborhood window (Windows 95, 98, or ME). Enable the master browsers to allow Windows clients outside of your server's subnet to access the server by name.

Setting Up Windows Clients for TCP/IP Networking

To have access to Windows services, Windows client computers must be properly configured to connect over TCP/IP. See your Windows networking documentation for information on TCP/IP configuration.

Connecting for File Service From Windows

A Windows user can connect to the Windows file service of Mac OS X Server by using My Network Places in Windows XP or 2000 or the Network Neighborhood in Windows 95, 98, or Millennium Edition (ME).

Before trying to connect to the server from a Windows client computer, find out the workgroup or domain of both the client computer and the file server. The procedure for doing this depends on the Windows version.

- For Windows XP, click Start, click Control Panel, click Performance and Maintenance, double-click the System icon, and then click the Computer Name tab.
- For Windows 2000, click Start, click Settings, click Control Panel, double-click the System icon, and then click the Network Identification tab.
- For Windows 95, 98, or ME, click Start, click Settings, click Control Panel, double-click the Network icon, and then click the Identification tab.

To find the server's workgroup name, open Server Admin, click Windows in the Computers & Services list, click Settings, then click General.

To connect to Windows file service from a Windows computer:

1. On the Windows client computer, open My Network Places (Windows XP or 2000) or the Network Neighborhood (Windows 95, 98, or ME). If you are in the same workgroup or domain as the server, skip to step 4.
2. Double-click the Entire Network icon.
3. Double-click the icon of the workgroup or domain the server is located in.
4. Double-click the server's icon.
5. Authenticate using the short name and password of a user account stored on the server.

   The user account can be stored in the server's local directory domain or its shared directory domain, if the server has one.

Connecting to the Server by Name or Address in Windows 95, 98, or ME

A Windows 95, 98, or Millennium Edition (ME) user can connect to Mac OS X Server for Windows file service without using the Network Neighborhood. This method requires knowing the server's IP address or its Windows computer name (also known as its NetBIOS name).

To connect to Windows file service without using the Network Neighborhood:

1. In Windows 95, 98, or ME, click Start, click Find, then click Computer.
2. Type the name or IP address of your Windows server.
3. Double-click the server to connect.
4. Authenticate using the short name and password of a user account stored on the server.

   The user account can be stored in the server's local directory domain or its shared directory domain, if the server has one.

Connecting to the Server by Name or Address in Windows XP

A Windows XP user can connect to Mac OS X Server for Windows file service without using My Network Places. This method requires knowing the server's IP address or its Windows computer name (also known as its NetBIOS name).

To connect to Windows file service without using My Network Places:

1. In Windows XP, click Start, click Search, click "Computers or people," then click "A computer on the network."
2. Type the name or IP address of your Windows server.
3. Double-click the server to connect.
4. Authenticate using the short name and password of a user account stored on the server.

   The user account can be stored in the server's local directory domain or its shared directory domain, if the server has one.

Setting Up Windows Clients for Print Service

To enable printing by Windows users who submit jobs using SMB, make sure Windows services are running and that one or more print queues are available for SMB use.

All Windows computers—including Windows 95, Windows 98, Windows Millennium Edition (ME), and Windows XP—support SMB for using printers on the network. Windows 2000 and Windows NT also support LPR.

Note: Third-party LPR drivers are available for Windows computers that do not have built-in LPR support.

Administering Windows Users, Groups, Computers, and Share Points

3

You can manage accounts for Windows users, groups of Windows users, and a computer list account for Windows workstations. You can also manage SMB share points.

User accounts, group accounts, computer accounts, and share points play a fundamental role in a server's day-to-day operations:

- A user account stores data Mac OS X Server needs for authenticating Windows users and providing Windows domain login, roaming user profiles, home directories, file service, mail service, and so on.
- A group account offers a simple way to control access to files and folders. A group account stores the identities of users who belong to the group.
- A computer account is a list of computers that are available to the same users and groups. The Windows Computers account lists the Windows workstations that have joined the Windows domain of the PDC—they are the Windows computers that can be used to log in to the Windows domain of the Mac OS X Server primary domain controller.
- A share point is a folder, hard disk, or hard disk partition that you make accessible over the network.

To make Windows services usable, Mac OS X Server needs to have accounts for Windows users, groups, and workstations. The server also needs share points for Windows services.

Setup Overview

Here is a summary of the major tasks you perform to set up users, groups, computers, and share points for Windows services. See the pages indicated for detailed information about each step.

Step 1: Set up share points (optional)
You share folders and volumes with users on the network by designating them as share points. On a server that is a PDC, share points are created automatically for roaming user profiles and home directories. You can set up alternate share points for home directories and user profiles on a PDC server or a domain member server. Additionally, you can set up other share points for files and folders that Windows users need to share. See "Managing SMB Share Points" on page 41.

Step 2: Set up user accounts
Each Windows user who will log in to the Windows domain must have a user account. A user who will not log in to the Windows domain but will use Windows file service or mail service must also have a user account. See "Managing Accounts for Windows Users" on this page.

Step 3: Join workstations to the Windows domain
If Windows workstations will be used for Windows domain login, they must join the Windows domain. You can set up Windows workstations to join the Mac OS X Server PDC just as you would set up workstations to join a Windows NT server's domain. For example, in Windows 2000 Professional or Windows XP Professional, you could use the Network Identification Wizard.

When a Windows workstation joins the PDC, Mac OS X Server automatically adds the workstation to the server's computer account named Windows Computers. You can also add workstations to this account by using Workgroup Manager. See "Managing Windows Workstations in the Windows Computers Account" on page 39.

Step 4: Set up group accounts for Windows users (optional)
You only need to do this if you want to use groups to set file permissions based on groups. Note that Mac OS X Server does not support NT-style ACLs. The differences: on Mac OS X Server, you can assign only a single group privilege (and a single individual user privilege) to a particular file or folder. On a Windows NT server, you can assign a wider range of permissions. See "Managing Groups for Windows Users" on page 38.

Managing Accounts for Windows Users

A user account stores data Mac OS X Server needs to validate a user's identity and provide services for the user, such as access to particular files on the server. If the user account resides on a server that is a primary domain controller (PDC) or on a server that is a member of a Windows domain governed by a PDC, the user account also enables someone using a Windows computer to log in to the Windows domain.

The same user account can be used to log in to a Mac OS X computer.

Where Windows User Accounts Are Stored

User accounts for Windows users can be stored in any directory domain accessible from the computer that needs to access the account. To be used for Windows domain login from a Windows computer, a user account must be stored in the LDAP directory domain of the Mac OS X Server that is the primary domain controller (PDC). A Windows user account that is not stored in the PDC's LDAP directory domain can be used to access other services. For example, a user account in the local directory domain of a Mac OS X Server can be used to access Windows file service provided by the same server.

See the Open Directory administration guide for complete information about the different kinds of directory domains.

Creating Windows User Accounts in the Primary Domain Controller

You can use Workgroup Manager to create a user account on a Mac OS X Server PDC. Windows users with accounts on a Mac OS X Server that is the primary domain controller (PDC) can log in to the Windows domain from a Windows workstation. These user accounts can also be used for other Windows services. You need administrator privileges for a directory domain to create a new user account in it.

To create a user account in the PDC:

1. In Workgroup Manager, click Accounts, then click the User button.
2. Open the LDAP directory domain and authenticate as an administrator of the domain.

   To open the LDAP directory domain, click the small globe icon above the list of users and choose from the pop-up menu.

   To authenticate, click the lock icon and enter the name and password of an administrator whose password type is Open Directory.
3. Choose Server > New User or click New User in the toolbar.
4. Specify settings for the user in the tabs provided.

   See "Working With Basic Settings for Users" on page 33 through "Working With Print Settings for Users" on page 37 for details.

   You can also use a preset or an import file to create a new user. For details, see the user management guide.

Creating Windows User Accounts in a Read/Write Directory Domain

You can use Workgroup Manager to create Windows user accounts in directory domains other than the LDAP directory domain of a server that is a primary domain controller. If Mac OS X Server provides Windows services, you can create Windows user accounts in the server's local directory domain. If this server is connected to an LDAP directory domain of another server, you can also create Windows user accounts in the other server's LDAP directory domain. The other server's LDAP directory domain must be configured for write access; it must not be read-only.

User accounts in the local directory domain or another server's LDAP directory domain cannot be used for Windows domain login. These user accounts can access other services, such as Windows file service, if the server that hosts the service has an authentication search policy that includes the directory domain in which the user account resides. For example, a Windows user account in the local directory domain of a server can access the Windows file service of the same server. For information on search policies, see the Open Directory administration guide.

To create a user account in a read/write directory domain:

1. Ensure that the directory services of the Mac OS X Server you're administering has been configured to access the domain of interest.

   Mac OS X Server can always access its own local directory domain. Use Directory Access to configure access to another server's LDAP directory domain. See the Open Directory administrator's guide for instructions.

2. In Workgroup Manager, click Accounts, then click the User button.
3. Open the directory domain in which you want to create user accounts, and authenticate as an administrator of the domain.

   To open a directory domain, click the small globe icon above the list of users and choose from the pop-up menu.

   To authenticate, click the lock icon and enter the name and password of an administrator of the directory domain. Authenticate as an administrator whose password type is Open Directory so you can create user accounts whose password type is also Open Directory, which is recommended for Windows user accounts.

4. Choose Server > New User or click New User in the toolbar.
5. Specify settings for the user in the tabs provided.

   See "Working With Basic Settings for Users" on page 33 through "Working With Print Settings for Users" on page 37 for details.

You can also use a preset or an import file to create a new user. For details, see the user management guide.

Editing Windows User Accounts

You can use Workgroup Manager to change a Windows user account. The account can reside on a Mac OS X Server that is the Windows primary domain controller (PDC) or in another directory domain.

To make changes to a user account:

1. Ensure that the directory services of the Mac OS X Server you're using has been configured to access the directory domain of interest.

   Mac OS X Server can always access its own local directory domain. A server that is a primary domain controller can access its own LDAP directory domain. To configure access to another server's LDAP directory domain, use Directory Access. See the Open Directory administrator's guide for instructions.

2. In Workgroup Manager, click Accounts, then click the User button.

3. Open the directory domain in which you want to edit user accounts, and authenticate as an administrator of the domain.

   To open a directory domain, click the small globe icon above the list of users and choose from the pop-up menu.

   To authenticate, click the lock icon and enter the name and password of an administrator of the directory domain. Authenticate as an administrator whose password type is Open Directory so you can edit user accounts whose password type is also Open Directory, which is recommended for Windows user accounts.

4. Select the account you want to edit.

5. Change settings for the user in the tabs provided.

   See "Working With Basic Settings for Users" (next) through "Working With Print Settings for Users" on page 37 for details.

Working With Basic Settings for Users

Basic settings are a collection of attributes that must be defined for all users. You work with basic settings in the Basic pane of a Workgroup Manager user account window. For detailed instructions on the following tasks, see the chapter on user accounts in the user management guide:

- Defining user names
- Defining short names
- Choosing stable short names
- Avoiding duplicate names
- Avoiding duplicate short names
- Defining user IDs
- Defining passwords
- Assigning administrator rights for a server
- Assigning administrator rights for a directory domain

Working With Windows Settings for Users

A user account that can be used to log in to a Windows domain has settings for a Windows home directory, a roaming user profile, and a Windows login script. You can work with these settings in the Windows pane of a Workgroup Manager user account window.

To configure Windows settings for a user account:

1. In Workgroup Manager, open the user account with which you want to work.

   To open an account, click the Accounts button, and then click the small globe icon below the toolbar and open the directory domain where the user's account resides. To edit the WIndows settings, click the lock to be authenticated, and then select the user in the user list.

2. Click Windows and change the settings as needed.

   User Profile Path: specifies the path to the user's profile. Leave this blank to use the default share point for user profiles, which is /Users/Profiles/ on the PDC server. (This SMB share point is not shown in Workgroup Manager.)

   To use a different share point for the user profile, enter the path using the universal naming convention (UNC) format:

   *servername**sharename**usershortname*

   where *servername* is the NetBIOS name of the PDC server or a Windows domain member server where you want the user share point stored; *sharename* is the name of the share point on the server; and *usershortname* is the first short name of the user account you're configuring. You can see the server's NetBIOS name by opening Server Admin, clicking Windows in the Computers & Services list, clicking Settings, clicking General, and looking at the Computer Name field.

   Login Script: specifies the relative path to a login script located in /etc/logon on the PDC server. For example, if an administrator places a script named setup.bat in /etc/logon, the Login Script field should contain "setup.bat".

   Hard Drive: specifies the drive letter that Windows maps to the user's home directory. If you leave this blank, drive letter H is used.

   Path: specifies the path to the user's home directory. Leave this blank to use the same home directory for Windows login and Mac OS X login, as specified on the Home pane of Workgroup Manager. You can also specify this home directory by entering a UNC path that doesn't include a share point: *servername**usershortname*.

   To specify a Windows home directory that is separate from the Mac OS X home directory, enter a UNC path that includes an SMB share point:

   *servername**sharepoint**usershortname*

You must make sure the specified share point is shared using SMB. Additionally, you must create the user's home directory folder in the share point. The folder you create must have the same name as the user's first short name. (Mac OS X Server automatically creates a home directory folder only in the share point specified on the Home pane.)

3 Click Save.

See "Setting Up a Home Directory for a Windows User" on page 36 and "Managing SMB Share Points" on page 41 for additional information.

Working With Advanced Settings for Users

Advanced settings include Mac OS X login settings, password validation policy, and a comment. You work with these settings in the Advanced pane of a Workgroup Manager user account window.

- User Password Type must be Open Directory or Shadow Password for Windows users.
- Settings at the top and bottom of the Advanced pane apply only when the user logs in from a Mac OS X computer. The following settings are not used for Windows services: "Allow simultaneous login," Login Shell, and Keywords.

For detailed instructions on changing advanced settings, see the chapter on user accounts in the user management guide.

Providing Secure Authentication for Windows Users

Mac OS X Server offers three secure ways to validate the passwords of Windows users:

- Open Directory Password Server
- Shadow password
- Crypt password with Authentication Manager enabled (a legacy technology)

Open Directory Password Server is the recommended approach. It stores passwords in a secure fashion, and it supports many authentication methods. Open Directory Password Server lets you implement password policies, and it supports user accounts in LDAP directories and legacy NetInfo domains.

A shadow password provides NT and LAN Manager authentication for user accounts stored in the local NetInfo domain. A Shadow password can be used to authenticate Windows file service provided by Mac OS X Server.

A crypt password with Authentication Manager enabled provides compatibility for user accounts on a server that has been upgraded from Mac OS X Server version 10.1. After upgrading the server to Mac OS X Server version 10.3, these user accounts should be changed to use Open Directory authentication, which is more secure than the legacy Authentication Manager. See the Open Directory administration guide for more information.

Working With Group Settings for Users

Group settings identify the groups a user is a member of. You work with these settings in the Groups pane of a Workgroup Manager user account window. For detailed instructions on the following tasks, see the chapter on user accounts in the user management guide:

- Defining a user's primary group
- Adding a user to groups
- Removing a user from a group
- Reviewing a user's group memberships

Setting Up a Home Directory for a Windows User

A Windows user can have a home directory for use when logging in to a Windows domain. Normally, this user can log in to a Mac OS X computer and use the same home directory.

You can create a home directory for a Windows user in any existing share point, or you can create the home directory in the /Users folder—a predefined share point. If you want to create a home directory in a new share point, create the share point first. See "Managing SMB Share Points" on page 41 for instructions.

For general information on home directories, see the chapter on home directories in the user management guide.

To create a home directory in an existing share point:

1. Make sure the share point has a mount record configured for home directories.

   In Workgroup Manager, click Sharing, click Share Points (on the left), select the share point in the list, click Network Mount (on the right), and make sure "Create a mount record for this share point" is selected and "For User Home Directories" is also selected. To change these settings, you must use the Where pop-up menu to choose the directory domain in which the user account resides, click the lock icon, and authenticate as an administrator of the directory domain.

2. In Workgroup Manager, open the user account for which you want to create a home directory.

   To open an account, click the Accounts button, and then click the small globe icon below the toolbar and open the directory domain where the user's account resides. To edit the home directory information, click the lock to be authenticated, and then select the user in the user list.

3. Click Home.

4. In the share points list, select /Users or the share point you want to use.

5. Click Create Home Now, and then click Save.

After creating a home directory for a Windows user, make sure the settings in the Windows pane are configured correctly. See "Working With Windows Settings for Users" on page 34 for instructions.

Working With Mail Settings for Users

A Windows user can have a Mac OS X Server mail service account. You create a mail service account for a user by specifying mail settings for the user in the Mail pane of a Workgroup Manager user account window. For detailed instructions on the following tasks, see the chapter on user accounts in the user management guide:

- Disabling a user's mail service
- Enabling mail service account options
- Forwarding a user's mail

To use a mail service account, the user simply configures a mail client to identify the user name, password, mail service, and mail protocol you specify in the Mail pane.

See the mail service administration guide for information about how to set up and manage Mac OS X Server mail service.

Working With Print Settings for Users

Print settings associated with a user's account define the ability of a user to print to accessible Mac OS X Server print queues for which print service enforces print quotas. The print service administration guide tells you how to set up quota-enforcing print queues.

You work with a user's print quotas in the Print pane of a user account window in Workgroup Manager:

- By default, a user has access to none of the print queues that enforce print quotas.
- You can allow a user access to all print queues that enforce quotas.
- You can let a user print to specific print queues that enforce quotas.

For detailed instructions on working with print settings for users, see the chapter on user accounts in the user management guide.

Defining a Guest User

You can set up Windows services and some other services to support anonymous users, who don't have user accounts. These guest users can't be authenticated because they don't have user names and passwords. You do not have to create a user account of any kind to support guest users.

The following services can support guest access:

- Windows file, print, browsing, and name resolution services (for setup information, see "Allowing Guest Access for Windows Services" on page 55)
- Apple file service (for setup information, see the file services administration guide)
- FTP service (for setup information, see the file services administration guide)

- Web service (for setup information, see the web technologies administration guide)

Users who connect to a server anonymously are restricted to files, folders, and websites with privileges accorded to Everyone.

Deleting a Windows User Account

You can use Workgroup Manager to delete a user account from a directory domain of Mac OS X Server.

To delete a user account using Workgroup Manager:

1. In Workgroup Manager, click the Accounts button, then click the User button.
2. Open the directory domain that contains the user account you want to delete, and authenticate as an administrator of the domain.

   To open a directory domain, click the small globe icon above the list of users and choose from the pop-up menu.
3. Select the account you want to delete, then choose Server > Delete Selected User.

Disabling a Windows User Account

To disable a Windows user account, you can

- Deselect the "User can log in" option on the Basic pane in Workgroup Manager.
- For a user account whose password type is Open Directory, set a password policy that disables login. For instructions, see the user authentication chapter of the Open Directory administration guide.
- Delete the account. For instructions, see the previous task, "Deleting a Windows User Account."
- Change the user's password to an unknown value. For instructions, see "Working With Basic Settings for Users" on page 33.

Managing Groups for Windows Users

A group account offers a simple way to manage a collection of users with similar needs. A group account stores the identities of users who belong to the group and other information that applies only to Mac OS X users. Although some group information doesn't apply to Windows users, you can add Windows users to groups that you create. A group can be assigned special access privileges to files and folders, as described in the file services administration guide.

The procedures for managing group accounts are the same for groups whose members include Windows users as for groups that contain only Mac OS X users. You use Workgroup Manager to administer group accounts. For detailed instructions on the following tasks, see the chapter on group accounts in the user management guide:

- Creating group accounts
- Editing group account information
- Adding users to a group

- Removing users from a group
- Naming a group
- Defining a group ID
- Deleting a group account

Working With Group Folder Settings for Windows Groups

If you use the Group Folder pane in Workgroup Manager to set up a folder for members of a particular group, the group folder isn't mounted automatically on Windows workstations when group members log in to the Windows domain. If the group folder's share point is shared using SMB, a Windows user can go to My Network Places (or Network Neighborhood) and access the contents of the group folder. For more information on group folders, see the chapter on group accounts in the user management guide.

Managing Windows Workstations in the Windows Computers Account

Every Windows computer supported by the Mac OS X Server primary domain controller must be part of the Windows Computers account. Adding a computer to a computer account creates a computer record for the computer. The computer record identifies the Windows computer by its NetBIOS name. The computer record for a Windows computer also contains information for authenticating the computer as a trusted workstation in the Windows domain. Mac OS X Server creates this information (a UID and a GID) for each computer you add to the Windows Computers account.

For general information on computer accounts and adding computers to them, see the chapter on computer accounts in the user management guide.

Adding Computers to the Windows Computers Account

A Mac OS X Server PDC automatically adds a Windows computer to the server's Windows Computers account when the computer joins the PDC's Windows domain, but you can also use Workgroup Manager to add computers to the Windows Computers account.

To add computers to the Windows Computer list:

1. In Workgroup Manager, click Accounts, then click the Computers button.
2. Open the LDAP directory domain and authenticate as an administrator of the domain.

   To open the LDAP directory domain, click the small globe icon above the list of computers and choose from the pop-up menu.

   To authenticate, click the lock icon and enter the name and password of a directory domain administrator.
3. Click List, then select Windows Computers in the list of computer accounts.

4 Click the Add button, enter the computer's NetBIOS name and an optional description, and click Add.

5 Click Save.

6 Continue adding computers until your list is complete.

Removing Computers From the Windows Computers Account

Using Workgroup Manager, you can remove one or more computers from the Windows Computers account of a Mac OS X Server primary domain controller (PDC). When you delete a computer from the Windows Computers account, the computer can no longer be used for logging in to the PDC.

To remove computers from the Windows Computer list:

1 In Workgroup Manager, click Accounts, then click the Computers button.

2 Open the LDAP directory domain and authenticate as an administrator of the domain.

To open the LDAP directory domain, click the small globe icon above the list of computers and choose from the pop-up menu.

To authenticate, click the lock icon and enter the name and password of a directory domain administrator.

3 Click List, then select Windows Computers in the list of computer accounts.

4 In the List pane, select one or more computers in that account's computer list.

To select multiple computers, Command-click or Shift-click in the list.

5 Click Remove, then click Save.

Editing Information About a Computer in the Windows Computers Account

If you want to change the name or description of a computer in the Windows Computers account, use Workgroup Manager to remove the computer and then add the computer back with the revised information.

Moving a Windows Computer to a Different Computer Account

You cannot move a Windows computer from the Windows Computers account to a different account. Windows computers must be part of the Windows Computers account, and computers cannot belong to more than one account.

Deleting the Windows Computers Account

The Windows Computers account cannot be deleted.

Managing SMB Share Points

Share points for Windows home directories and roaming user profiles are set up automatically on a Mac OS X Server primary domain controller (PDC), but you can set up other share points. Windows uses the server message block (SMB) protocol to access share points.

The default share point for Windows home directories is the same as the share point for Mac OS X home directories. The default share point for user profiles is the /Users/Profiles/ folder on the PDC server. (This SMB share point is not shown in Workgroup Manager.) You can set up alternate SMB share points for home directories and user profiles on the PDC server or on domain member servers.

You can set up additional share points for exclusive or nonexclusive use of Windows users. For example, you could set up a share point where Windows and Mac OS users save shared graphics or word processing files that can be used on either platform. Conversely, you could set up a share point for SMB access only, so that Windows users have a network location for files that can't be used on other platforms.

For an overview of share points, including a discussion of issues you may want to consider before creating them, see the share points chapter in the file services administration guide.

Opportunistic Locking (oplocks)

SMB share points in Mac OS X Server support the improved performance offered by opportunistic locking ("oplocks").

In general, file locking prevents multiple clients from modifying the same information at the same time; a client locks the file or part of the file to gain exclusive access. Opportunistic locking grants this exclusive access but also allows the client to cache its changes locally (on the client computer) for improved performance.

To enable oplocks, you change the Windows protocol settings for a share point using Workgroup Manager.

Important: Do not enable oplocks for a share point that's using any protocol other than SMB.

Strict Locking

It's normally the responsibility of a client application to see if a file is locked before it tries to open it. A poorly written application may fail to check for locks, and could corrupt a file already being used by someone else.

Strict locking, which is enabled by default, helps prevent this. When strict locking is enabled, the SMB server itself checks for and enforces file locks.

Creating an SMB Share Point and Setting Privileges

You use the Sharing module of Workgroup Manager to share volumes (including disks, CDs and DVDs), partitions, and individual folders by setting up share points. When you create a share point, you can configure it to be shared using any combination of the AFP, FTP, SMB, and NFS protocols. You can also control access to the share point and its contents by setting access privileges.

Note: Don't use a slash (/) in the name of a folder or volume you plan to share. Users trying to access the share point might have trouble seeing it.

To create an SMB share point and set privileges:

1. Open Workgroup Manager and click Sharing.
2. Click All and select the item you want to share.
3. Click General.
4. Select "Share this item and its contents."
5. To control who has access to the share point, change the owner or group of the shared item. Type names or drag names from the Users & Groups drawer.

   To open the drawer, click Users & Groups. If you don't see a recently created user or group, click Refresh. To change the autorefresh interval, choose Workgroup Manager > Preferences.
6. Use the pop-up menus next to the fields to change the privileges for the Owner, Group, and Everyone.

   Everyone is any user who can log in to the file server: registered users and guests.
7. (Optional) To apply the ownership and privileges of the share point to all files and folders it contains, click Copy. This overrides privileges that other users may have set.
8. Click Protocols (on the right) and choose Windows File Settings from the pop-up menu.
9. To provide SMB access to the share point, select "Share this item using SMB."
10. To allow unregistered users access to the share point, select "Allow SMB guest access."

    For greater security, don't select this item.
11. To change the name that clients see when they browse for and connect to the share point using SMB, type a new name in the "Custom SMB name" field.

    Changing the custom SMB name doesn't affect the name of the share point itself, only the name that SMB clients see.
12. To allow clients to use opportunistic file locking, select "Enable oplock."

    Do not enable oplocks for a share point that's using any protocol other than SMB. For more information on oplocks, see "Opportunistic Locking (oplocks)" on page 41.

    To have clients use standard locks on server files, select "Enable strict locking."

13 Choose a method for assigning default access privileges for new files and folders in the share point.

To have new items adopt the privileges of the enclosing item, select "Inherit permissions from parent."

To assign specific privileges, select "Assign as follows" and set the Owner, Group, and Everyone privileges using the pop-up menus.

14 To prevent AFP access to the new share point, choose Apple File Settings from the pop-up menu and deselect "Share this item using AFP."

15 To prevent FTP access to the new share point, choose FTP Settings from the pop-up menu and deselect "Share this item using FTP."

16 To prevent NFS access to the new share point, choose NFS Export Settings from the pop-up menu and deselect "Export this item and its contents to."

17 Click Save.

From the Command Line

You can also set up a share point using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing Windows (SMB) Settings for a Share Point

You can use Workgroup Manager to set whether a share point is available via SMB and to change settings such as the share point name that SMB clients see, whether guest access is allowed, whether opportunistic locking is allowed, and the default privileges for new items.

To change the settings of an SMB share point:

1 Open Workgroup Manager and click Sharing.

2 Click Share Points and select the share point.

3 Click Protocols (on the right) and choose Windows File Settings from the pop-up menu.

4 To provide SMB access to the share point, select "Share this item using SMB."

5 To allow unregistered users access to the share point, select "Allow SMB guest access."

For greater security, don't select this item.

6 To change the name that clients see when they browse for and connect to the share point using SMB, type a new name in the "Custom SMB name" field.

Changing the custom SMB name doesn't affect the name of the share point itself, only the name that SMB clients see.

7 To allow clients to use opportunistic file locking, select "Enable oplock."

To have clients use standard locks on server files, select "Enable strict locking."

Do not enable oplocks for a share point that's using any protocol other than SMB. For more information on oplocks, see "Opportunistic Locking (oplocks)" on page 41.

8 Choose a method for assigning default access privileges for new files and folders in the share point.

To have new items adopt the privileges of the enclosing item, select "Inherit permissions from parent."

To assign specific privileges, select "Assign as follows" and set the Owner, Group, and Everyone privileges using the pop-up menus.

9 Click Save.

From the Command Line

You can also change a share point's SMB settings using the `sharing` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Managing Share Points

For information on typical day-to-day tasks you might perform after you have set up share points on your server, see the chapter on share points in the file services administration guide. It describes the following tasks:

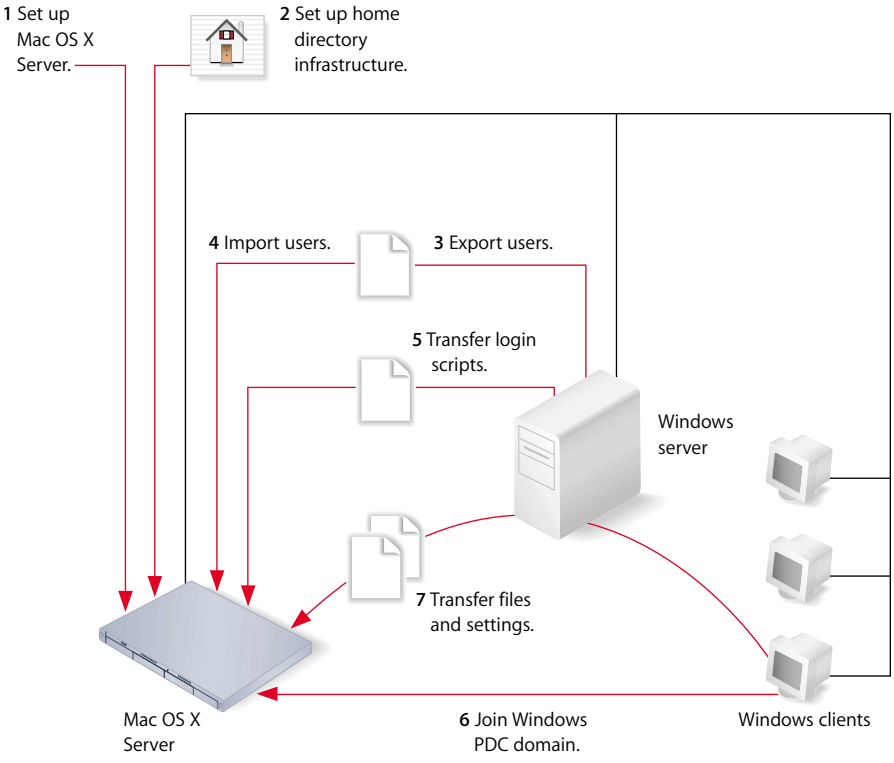
- Disabling a share point
- Disabling a protocol for a share point
- Viewing share points
- Copying privileges to enclosed items
- Viewing share point settings
- Changing share point owner and privilege settings
- Changing NFS share point client scope
- Allowing guest access to a share point
- Setting up a drop box

Migrating Users From a Windows Server to Mac OS X Server

4

You can set up Mac OS X Server user accounts and home directories to replace those on existing Windows NT, Windows 2000, or Windows 2003 servers.

The following picture summarizes the steps that follow it.


1 Set up Mac OS X Server.
2 Set up home directory infrastructure.
4 Import users.
3 Export users.
5 Transfer login scripts.
Windows server
7 Transfer files and settings.
Mac OS X Server
6 Join Windows PDC domain.
Windows clients

Step 1: Set up Mac OS X Server

Follow the instructions in the getting started guide:

1. Install server software.
2. Perform initial server setup, making sure that you create an Open Directory master domain and a Windows primary domain controller (PDC) on the server. The Windows PDC lets Windows NT, Windows 2000, and Windows XP workstation users log in to the PDC, change passwords during login, and have roaming user profiles and network home directories on Mac OS X Server.

   In Server Assistant's Directory Usage pane, choose Open Directory Master from the "Set directory usage to" pop-up menu. Then select Enable Windows Primary Domain Controller and enter a computer name and domain/workgroup name:

   In the Computer Name field, enter the name you want Windows users to see when they connect to the server. This is the server's NetBIOS name. The name should contain no more than 15 characters, no special characters, and no punctuation. If practical, make the server name match its unqualified DNS host name. For example, if your DNS server has an entry for your server as "server.example.com," give your server the name "server."

   In the Domain/Workgroup field, enter the name of the Windows domain that the server will host. The domain name cannot exceed 15 characters.

Step 2: Set up the home directory infrastructure

When you import users, you identify a location for their home directories. You can use one of the predefined share points, such as the /Users folder. Or you can set up your own share point.

1. If you use a predefined share point, select it in Workgroup Manager and go to step 3 in this sequence. Otherwise, use step 2 first.

   To select a predefined share point in Workgroup Manager, click Sharing. Click Share Points and select the share point.
2. If you want to set up your own share point on Mac OS X Server, create the folder you want to serve as the home directory share point and then use Workgroup Manager to make the folder a share point.

   In Workgroup Manager, click Sharing. Click All and select the folder. Click General and select "Share this item and its contents." Set up the privileges, and then click Save. Click Protocols and make sure the folder is shared using AFP or NFS. Click Save again.
3. Set up the share point to mount automatically on client workstations.

   With the share point selected in Workgroup Manager, click Network Mount. Choose the PDC server's LDAP directory from the Where pop-up menu. Click the lock to the right of this pop-up menu and authenticate as an administrator of the LDAP directory. Select "Create a mount record for this share point." Choose AFP or NFS from the Protocol pop-up menu. Select "Use For User Home Directories" and click Save.

4 Set up default file access permissions for Windows users.

Click Protocols, choose Windows File Settings from the pop-up menu, and specify permissions under "Default permissions for new files and folders." Click Save.

Step 3: Export users from the Windows server domain

1 Open the user management application (such as User Manager for Windows NT 4.0 server) on your Windows server.

2 Export users into a tab-delimited file.

Long names and short names are exported. On Windows NT, these correspond to name and user name, respectively. For Windows 2000 Active Directory, they correspond to name and pre-windows 2000 logon name, respectively.

Step 4: Import users on Mac OS X Server

1 Make sure that Windows services are running.

Open Server Admin, select Windows in the Computers & Services list, and click Start Service if required.

2 On the Windows server, map a network drive to Mac OS X Server.

3 Log in as the administrator user you defined when setting up Mac OS X Server.

4 Copy the export file to Mac OS X Server.

5 On Mac OS X Server, modify the export file:

a Change the Windows line endings to UNIX line endings. You can use the vi command-line editor to do this. The following command opens vi for a file named MyFile with line endings set to UNIX style:

```
vi -c "set fileformat=unix" MyFile
```

b Remove the header inserted during export.

c Reorder the columns so that the short name appears first. A spreadsheet application is useful for this type of editing.

d Add the following header as the first line of the file:

```
0x0D 0x5C 0x09 0x2C dsRecTypeStandard:Users 2
dsAttrTypeStandard:RecordName dsAttrTypeStandard:RealName
```

6 Open Workgroup Manager. Make sure the Accounts button is selected in the toolbar and the Users button is selected above the list of accounts (on the left). The PDC server's LDAP directory should be the current directory domain. If it's not, click the small globe beneath the toolbar to select the server's LDAP directory.

7 Define a user account preset in the server's LDAP directory. The settings you associate with a preset are assigned to each imported user, simplifying the definition of user profile path, login script, home directory share point, and other values.

Click New User, and specify values you want all imported Windows users to inherit. For details about how to work with most of the user settings, see the user management guide. See "Managing Accounts for Windows Users" on page 30 for details about Windows user settings.

Set up password options so that users are forced to change their passwords the next time they log in. Using this approach means you don't have to individually specify passwords for each user in the export file or in Workgroup Manager after importing the users. To access password option settings, click Advanced, then Options.

When you are finished specifying values, choose Save Preset from the Presets pop-up menu.

8 In Workgroup Manager, choose Server > Import.

9 Navigate to the user export file and select it. Then choose a duplicate handling option, identify the preset you want to use, and optionally supply a first user ID and a primary group ID.

10 Click Import.

11 Optionally define group accounts for controlling access to files.

On Mac OS X computers, file and folder access permissions (Read & Write, Read only, Write only, or No Access) are specified for an owner (a user), a group, and all users, known as "Everyone." Mac OS X Server does not support access control lists (ACLs). Additional groups can be used to set up group-level permissions for files transferred from the Windows server.

To define a group, select the group list in Workgroup Manager, click New Group, and enter group names and a group ID. To add users to the group, click Add (+), select the users you want to belong to the group, and drag selected users to the Members list.

Step 5: Transfer login scripts to Mac OS X Server

1 Copy login scripts from the Windows server to /etc/netlogon/ on Mac OS X Server.

2 In Workgroup Manager, select each Windows PDC user and make sure that the location of the login script is correctly specified. The Login Script field should contain the relative path to a login script located in /etc/logon/. For example, if you've copied a script named setup.bat into /etc/logon/, the Login Script field should contain setup.bat.

Step 6: Join Windows clients to Mac OS X Server PDC

On the workstation of each Windows user for whom you created an account on Mac OS X Server, join the Windows PDC domain on the server to enable Open Directory authentication for users who log in at the workstation.

Now when a Windows workstation user logs in to Mac OS X Server, his or her home directory is automatically created and mounts on the Windows workstation.

Step 7: Transfer client files and settings to Mac OS X Server home directories

Each Windows workstation user can now move files from the Windows server to his or her home directory on Mac OS X Server.

1. On a Windows client that's been set up to join the Mac OS X Server domain, map a network drive to Mac OS X Server and log in as one of the imported users.

   The first time a Windows user logs in, his or her home directory mounts on the Windows workstation.

2. Map a network drive to the Windows server where the files to transfer reside.
3. Copy files of interest to the Mac OS X Server home directory. Default permissions set up in step 2 are assigned to each file.

   When you log out, user settings (such as the background picture) are saved on Mac OS X Server and used for future login.

Managing Windows Services

5

You can use Server Admin to start and stop Windows services, monitor them, change their server's Windows identity, manage access to them, manage their logs, and change their advanced settings.

For management task descriptions and instructions, see:

- "Starting and Stopping Windows Services" on this page
- "Monitoring Windows Services" on page 52
- "Changing the Server's Windows Identity" on page 54
- "Managing Access to Windows Services" on page 55
- "Managing Windows Services Logging" on page 56
- "Managing Advanced Windows Services Settings" on page 57

Starting and Stopping Windows Services

You can start and stop Windows services.

Starting Windows Services

You can use Server Admin to start Windows services if they are stopped.

To start Windows services:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Start Service.

From the Command Line

You can also start Windows services by using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Stopping Windows Services

You can use Server Admin to stop Windows services.

Important: When you stop Windows services, connected users will lose any information they haven't saved.

To stop Windows services:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Stop Service.

From the Command Line

You can also stop Windows services by using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Monitoring Windows Services

You can check the status of Windows services, view the Windows services logs, and see a list of users who are currently connected for Windows services.

Viewing Windows Services Status

You can use Server Admin to check the status of Windows services.

To view Windows services status:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Overview to see whether the service is running and how many users are connected.
3. Click Logs to see the Windows file service and name service logs.

   Use the Show pop-up menu to choose which log to view.
4. Click Connections to see a list of the users currently connected to the Windows services.

   The list includes the users' names, IP addresses, and duration of connections. A button at the bottom of the pane lets you disconnect a user.
5. Click Graphs to see graphs of connected users or throughput.

   Use the slider to adjust the time scale.

From the Command Line

You can also check Windows services status by using the `serveradmin` command in Terminal or using the `cat` or `tail` command to view the log files in /var/log/samba. For more information, see the file services chapter of the command-line administration guide.

Viewing Windows Services Logs

You can use Server Admin to view the logs of Windows services.

To view Windows services logs:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Logs to see the Windows file service and name service logs.
3. Use the Show pop-up menu to choose which log to view.

From the Command Line

You can also view the logs of Windows services by using the `cat` or `tail` command in Terminal to view the log files in /var/log/samba. For more information, see the file services chapter of the command-line administration guide.

Viewing Windows Services Connections

You can use Server Admin to see which users are connected to Windows services, and you can forcibly disconnect users.

Important: Users who are disconnected will lose unsaved work in open files.

To view Windows services connections:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Connections to see a list of the users currently connected to the Windows services.

   The list includes the users' names, IP addresses, and duration of connections.

   A button at the bottom of the pane lets you disconnect a user.

From the Command Line

You can also check the number of connections to Windows services by using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Viewing Windows Services Graphs

You can use Server Admin to view graphs of connected Windows users or the throughput of Windows services.

To view Windows services graphs:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Graphs to see graphs of connected users or throughput.
3. Use the slider to adjust the time scale.

Disconnecting Windows Users

You can use Server Admin to forcibly disconnect users of Windows services.

Important: Users who are disconnected will lose unsaved work in open files.

To forcibly disconnect users of Windows services:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Connections to see a list of the users currently connected to the Windows services.

   The list includes the users' names, IP addresses, and duration of connections.
3. Select users that you want to forcibly disconnect and click Disconnect.

Changing the Server's Windows Identity

You can change a server's identity among clients of Windows services by changing the server's Windows computer name or by changing its Windows domain or workgroup.

Changing the Server's Windows Computer Name

Using Server Admin, you can change the computer name by which Mac OS X Server is known in a Windows domain or workgroup. If the server is the primary domain controller (PDC) or a Windows domain member, the computer name is the server's NetBIOS name in the domain. If the server provides standalone Windows services but is not the PDC or a domain member, the computer name is the server's NetBIOS name in the workgroup. Windows users see this name when they connect to the server.

To change the Windows computer name of Mac OS X Server:

1. In Server Admin's Computers & Services list, select Windows for the server whose Windows computer name you want to change.
2. Click Settings (near the bottom of the window), then click General (near the top).
3. Enter the computer name, then click Save.

   The name should contain no more than 15 characters, no special characters, and no punctuation. If practical, make the server name match its unqualified DNS host name. For example, if your DNS server has an entry for your server as "server.example.com," give your server the name "server."
4. If the server is the PDC or a Windows domain member, you must authenticate by entering the name and password of a user account that can administer the LDAP directory domain on the PDC server.

   Since workgroups are ad hoc, you do not have to authenticate as an administrator to change the computer name of a server that provides only standalone Windows services.

From the Command Line

You can also change the server name using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Changing the Server's Windows Domain

Using Server Admin, you change the Windows domain of a server that is a domain member.

> *Warning:* Do not change the domain name of a PDC server unless absolutely necessary. If you change the name of the PDC domain, Windows workstations that were domain members will have to rejoin the domain under its new name.

To change the Windows domain of Mac OS X Server:

1. In Server Admin's Computers & Services list, select Windows for the server whose Windows domain you want to change.
2. Click Settings (near the bottom of the window), then click General (near the top).
3. Enter the Windows domain name, then click Save.

Changing the Sever's Windows Workgroup

Using Server Admin, you can change the workgroup name of a server that provides only standalone Windows services (file, print, browsing, or WINS). Windows users see the workgroup name in the Network Neighborhood window. If you have Windows domains on your subnet, use one of them as the workgroup name to make it easier for clients to communicate across subnets. Otherwise, consult your Windows network administrator for the correct name.

To change the Windows workgroup name of Mac OS X Server:

1. In Server Admin's Computers & Services list, select Windows for the server whose Windows domain you want to change.
2. Click Settings (near the bottom of the window), then click General (near the top).
3. Type a name in the Workgroup field, then click Save.

From the Command Line

You can also change the Windows workgroup name using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Managing Access to Windows Services

You can manage access to Windows services by allowing or disallowing guest access to Windows file service and by limiting the number of connected Windows clients.

Allowing Guest Access for Windows Services

You can use Server Admin to enable or disable guest access to Windows file service. Guest users can access Windows file service on your server without supplying a name and password. For better security, do not allow guest access.

Users must always enter a name and password to log in to the Windows domain of a Mac OS X Server primary domain controller from a Windows workstation. The Windows print service provided by Mac OS X Server does not require authentication. Windows browsing and name resolution services do not require authentication either.

To enable guest access to Windows file service:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Settings, then click Access.
3. Click "Allow Guest access," then click Save.

   If "Allow Guest access" is selected, users can connect for Windows file service without using a name or password.

   If "Allow Guest access" is unselected, users must supply a valid name and password to use Windows file service.

From the Command Line

You can also enable or disable guest access to Windows file service using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Limiting the Number of Connected Windows Clients

Using Server Admin, you can limit the potential resources consumed by Windows services by limiting the maximum number of connections.

To set the maximum number of connections:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Settings, then click Access.
3. Select "__maximum" and type the maximum number of connections.
4. Click Save.

From the Command Line

You can also limit client connections by using the `serveradmin` command in Terminal to limit the number of SMB processes. For more information, see the file services chapter of the command-line administration guide.

Managing Windows Services Logging

Using Server Admin, you can choose the level of detail you want to log for Windows services.

To specify log contents:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Settings, then click Logging (near the top).

3 Choose from the Log Detail pop-up menu to set the level of detail you want to record, then click Save.

The more detailed the logging, the larger the log file.

The following table shows the level of detail you get for each option.

Events logged	Low	Medium	High
Warnings and errors	Yes	Yes	Yes
Service startup and stop		Yes	Yes
User login failures		Yes	Yes
Browser name registrations		Yes	Yes
File access events			Yes

From the Command Line

You can also change Windows services logging settings using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Managing Advanced Windows Services Settings

You can use the Advanced pane of Windows services settings in Server Admin to choose a client code page, set the server to be a workgroup or domain master browser, specify the server's WINS registration, and enable virtual share points for user homes.

Changing the Windows Code Page

You can use Server Admin to change the *code page,* which determines the character set used for Windows services.

To change the Windows code page:

1 Open Server Admin and select Windows in the Computers & Services list.

2 Click Settings, then click Advanced.

3 Choose the character set you want clients to use from the Code Page pop-up menu, then click Save.

From the Command Line

You can also change the Windows code page by using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Enabling Windows Domain Browsing

If there are no Microsoft servers on your subnet or network to control domain browsing, you can use these options to restrict domain browsing to a single subnet or allow browsing across your network.

To enable domain browsing:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Settings, then click Advanced.
3. Next to Services, select Workgroup Master Browser, Domain Master Browser, or both.

   Select Master Browser to let clients browse for and locate servers in a single subnet.

   Select Domain Master Browser to let clients browse for and locate servers across your network (subnets).
4. Click Save.

From the Command Line

You can also change Windows domain browsing settings by using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Registering With a WINS Server

Windows Internet Naming Service (WINS) matches server names with IP addresses. You can use your server as the local name resolution server, or you can register with an external WINS server.

To register your server with a WINS server:

1. Open Server Admin and select Windows in the Computers & Services list.
2. Click Settings, then click Advanced.
3. Select one of the options under WINS Registration.

   Choose "Off" to prevent your server from registering itself with any external WINS server or local name resolution server.

   Choose "Enable WINS server" to have the file server provide local name resolution services. This allows clients across multiple subnets to perform name/address resolution.

   Choose "Register with WINS server" if your Windows clients and Windows server are not all on the same subnet, and your network has a WINS server. Then enter the IP address or DNS name of the WINS server.
4. Click Save.

From the Command Line

You can also change WINS settings using the `serveradmin` command in Terminal. For more information, see the file services chapter of the command-line administration guide.

Solving Problems With Windows Services

6

If you encounter problems while working with Windows services of Mac OS X Server, you might find a solution in this chapter.

Problems are listed in the following categories:

- Problems with a primary domain controller
- Problems with Windows file service
- Problems with Windows print service

Problems With a Primary Domain Controller

Problems with a primary domain controller (PDC) can have several causes.

User Can't Log in to the Windows Domain

- Make sure the user account is configured to use Open Directory authentication. If the user account was created in a previous version of Mac OS X Server (version 10.1 or earlier) and is still configured to use Authentication Manager (the password type is "Crypt password"), change the account to use Open Directory authentication.
- Make sure the workstation has joined the PDC domain

Windows User Has No Home Directory

- Make sure the correct home directory location is selected on the Home pane of Workgroup Manger.
- Make sure the home directory path is correct on the Windows pane of Workgroup Manger.
- Using Server Admin, connect to the server where the user's home directory resides. Select Windows in the Computers & Services list, click Advanced, and make sure the "Enable virtual share points" setting is selected.
- The drive letter chosen for the user may be conflicting with a drive letter that's already in use on the Windows workstation. Remedy: change either the drive letter setting on the Windows pane of Workgroup Manager or the mappings of other drive letters on the workstation.

Windows User's Profile Settings Revert to Defaults

- Make sure the correct home directory location is selected on the Home pane of Workgroup Manger.
- Make sure the home directory path is correct on the Windows pane of Workgroup Manger.
- The drive letter chosen for the user may be conflicting with a drive letter that's already in use on the Windows workstation. Remedy: change either the drive letter setting on the Windows pane of Workgroup Manager or the mappings of other drive letters on the workstation.

Windows User Loses Contents of My Documents Folder

- Make sure the correct home directory location is selected on the Home pane of Workgroup Manger.
- Make sure the user profile path is correct on the Windows pane of Workgroup Manger. The contents of My Documents are stored in the user profile.
- The drive letter chosen for the user may be conflicting with a drive letter that's already in use on the Windows workstation. Remedy: change either the drive letter setting on the Windows pane of Workgroup Manager or the mappings of other drive letters on the workstation.

Problems With Windows File Service

You can solve some common problems with Windows file service and with file services in general.

User Can't Authenticate for Windows File Service

If a user can't authenticate for Windows file service, make sure the user account is configured to use Open Directory authentication. If the user account was created in a previous version of Mac OS X Server (version 10.1 or earlier) and is still configured to use Authentication Manager, change the account to use Open Directory authentication. You do this in the Advanced pane of a user account window in Workgroup Manager.

User Can't See the Windows Server in the Network Neighborhood

- Make sure the user's computer is properly configured for TCP/IP and has the appropriate Windows networking software installed.
- Go to the DOS prompt on the client computer and type "ping *IP address*" where *IP address* is your server's address. If the ping fails, then there is a TCP/IP network problem.
- If the user's computer is on a different subnet from the server, try the following:
  - Make sure the "Enable WINS server" option is selected or the "Register with WINS server" option is selected and configured correctly. These options are in the Settings pane of Windows services in Server Admin.

- On the Windows computer, choose View > Refresh to force Windows to discover newly added network resources, which can otherwise take several minutes to be discovered.
- On the Windows computer, map a Mac OS X Server share point to a drive letter. You can do this by opening the Network Neighborhood and choosing Tools > Map Network Drive.

Note: If Windows computers are properly configured for networking and connected to the network, client users can connect to the Windows file service of Mac OS X Server even if they can't see the server icon in the Network Neighborhood window.

General Problems With File Services

For possible solutions to the following additional file services problems, see the chapter on solving problems in the file services administration guide.

- Users can't find a shared item
- Users can't see the contents of a share point
- You can't find a volume or directory to use as a share point

Problems With Windows Print Service

You can solve some common problems with Windows print service and with print services in general.

Windows Users Can't Print

If Windows NT 4.x clients can't print to the server, make sure that the queue name is not the TCP/IP address of the printer or server. Use the DNS host name instead of the printer or server address or, if there is none, enter a queue name containing only letters and numbers.The name of an SMB print queue must not exceed 15 characters.

General Problems With Print Services

For additional problems and possible solutions, see the chapter on solving problems in the print service administration guide.

- Print service doesn't start
- Clients can't add queue
- Jobs in a server queue don't print
- Print queue becomes unavailable

Glossary

Active Directory The directory service of Microsoft Windows 2000 and 2003 servers.

administrator A user with server or directory domain administration privileges. Administrators are always members of the predefined "admin" group.

AFP (Apple Filing Protocol) A client/server protocol used by Apple file service on Macintosh-compatible computers to share files and network services. AFP uses TCP/IP and other protocols to communicate between computers on a network.

authentication The process of proving a user's identity, typically by validating a user name and password. Usually authentication occurs before an *authorization* process determines the user's level of access to a resource. For example, file service authorizes full access to folders and files that an authenticated user owns.

authorization The process by which a service determines whether it should grant a user access to a resource and how much access the service should allow the user to have. Usually authorization occurs after an *authentication* process proves the user's identity. For example, file service authorizes full access to folders and files that an authenticated user owns.

BSD (Berkeley System Distribution) A version of UNIX on which Mac OS X software is based.

code page Defines extensions to the character set for Microsoft Windows. The base character set, defined by the American Standard Code for Information Interchange (ASCII), maps letters of the Latin alphabet, numerals, punctuation, and control characters to the numbers 0 through 127. The code page maps additional characters, such as accented letters for a particular language and symbols, to the numbers 128 through 255.

computer account A list of computers that have the same preference settings and are available to the same users and groups.

directory domain A specialized database that stores authoritative information about users and network resources; the information is needed by system software and applications. The database is optimized to handle many requests for information and to find and retrieve information quickly. Also called a directory node or simply a directory.

FTP (File Transfer Protocol) A protocol that allows computers to transfer files over a network. FTP clients using any operating system that supports FTP can connect to a file server and download files, depending on their access privileges. Most Internet browsers and a number of freeware applications can be used to access an FTP server.

group A collection of users who have similar needs. Groups simplify the administration of shared resources.

guest user A user who can log in to your server without a user name or password.

home directory A folder for a user's personal use. Mac OS X also uses the home directory, for example, to store system preferences and managed user settings for Mac OS X users.

IP (Internet Protocol) Also known as IPv4. A method used with Transmission Control Protocol (TCP) to send data between computers over a local network or the Internet. IP delivers packets of data, while TCP keeps track of data packets.

IP address A unique numeric address that identifies a computer on the Internet.

LDAP (Lightweight Directory Access Protocol) A standard client-server protocol for accessing a directory domain.

local domain A directory domain that can be accessed only by the computer on which it resides.

Mac OS X The latest version of the Apple operating system. Mac OS X combines the reliability of UNIX with the ease of use of Macintosh.

Mac OS X Server An industrial-strength server platform that supports Mac, Windows, UNIX, and Linux clients out of the box and provides a suite of scalable workgroup and network services plus advanced remote management tools.

NetBIOS (Network Basic Input/Output System) A program that allows applications on different computers to communicate within a local area network.

NetInfo One of the Apple protocols for accessing a *directory domain*.

Open Directory The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use *LDAP, NetInfo,* or *Active Directory* protocols; *BSD* configuration files; and network services.

open source A term for the cooperative development of software by the Internet community. The basic principle is to involve as many people as possible in writing and debugging code by publishing the source code and encouraging the formation of a large community of developers who will submit modifications and enhancements.

Network File System (NFS) A client/server protocol that uses TCP/IP to allow remote users to access files as though they were local. NFS exports shared volumes to computers according to IP address, rather than user name and password.

print queue An orderly waiting area where print jobs wait until a printer is available. The print service in Mac OS X Server uses print queues on the server to facilitate management.

privileges Settings that define the kind of access users have to shared items. You can assign four types of privileges to a share point, folder, or file: read/write, read-only, write-only, and none (no access).

protocol A set of rules that determines how data is sent back and forth between two applications.

share point A folder, hard disk (or hard disk partition), or CD that is accessible over the network. A share point is the point of access at the top level of a group of shared items. Share points can be shared using *AFP,* Windows *SMB, NFS* (an "export"), or *FTP* protocols.

SMB (Server Message Block) A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. Windows services use SMB to provide access to servers, printers, and other network resources.

subnet A grouping on the same network of client computers that are organized by location (different floors of a building, for example) or by usage (all eighth-grade students, for example). The use of subnets simplifies administration.

TCP (Transmission Control Protocol) A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

WINS (Windows Internet Naming Service) A name resolution service used by Windows computers to match client names with IP addresses. A WINS server can be located on the local network or externally on the Internet.

workgroup A set of users for whom you define preferences and privileges as a group. Any preferences you define for a group are stored in the group account.

Index

A

advanced settings, Windows services 35
authentication
  Authentication Manager 19, 35
  crypt password 35
  domain member server 13, 21
  logging of failures 23
  Open Directory 59
  Open Directory Password Server 35
  PDC 19, 22
  print service 56
  shadow password 35
  VPN 13
  Windows services 18, 35
Authentication Manager 19, 35

B

basic settings 33

C

clients, Windows. *See* Windows clients, Windows workstations
code page, changing 57
computer account
  See also Windows Computers account
  defined 29
  Windows Computers 30, 39
computer name, changing 54
connections
  limiting 56
  Windows service, viewing 53
cross-platform issues for file service 18
crypt password 35

D

domain, changing 55
domain browsing 24, 57
domain login
  authentication 18
  PDC for 12, 22
  user accounts for 31

F

file service
  authenticating 18, 19
  connecting from Windows 26, 27
  guest access 23, 55
  log 52, 53
  problems 60
  providing 13

G

graphs, Windows services 53
group accounts
  defined 29
  group folder settings 39
  managing 38
  Windows users in 30
group folder 39
group settings, in user accounts 36
guest access
  file service 55
guest user 37

H

home directories
  accessing 12
  user account settings 36

L

locking
  SMB opportunistic 41
  SMB strict 41
login. *See* domain login
logs
  viewing 53
  Windows logging options 23, 57

M

Mac OS X Server
  administration applications 14
  documentation 8
mail settings, in user accounts 37
My Network Places, connecting from 26

N

naming share points 42
Network Neighborhood, connecting from 26

O

Open Directory Password Server 18, 35
oplocks. *See* opportunistic locking
opportunistic locking
  described 41
  enabling 42, 43

P

password validation. *See* authentication
PDC (primary domain controller)
  domain login 12
  home directories 12
  joining 13
  problems 59
  role 19
  setting up 22
  user profiles 12
print service
  configuring SMB sharing 25
  problems 61
  setting up a queue for Windows clients 25
  Windows clients 27
print settings, in user accounts 37
privileges, share points 42

R

roaming user profiles 12, 34

S

Server Admin 14
  allowing guest access to Windows services 56
  changing server's computer name 54
  changing server's Windows domain 55
  changing server's Windows workgroup 55
  changing the code page 57
  disconnecting Windows users 54
  enabling Windows service domain browsing 58
  enabling Windows services logs 56
  limiting connections to Windows services 56
  monitoring Windows services 52
  registering Windows service with WINS 58
  starting Windows services 25
  stopping Windows services 52
  viewing Windows services connections 53
  viewing Windows services graphs 53
  viewing Windows services logs 53
  Windows services Advanced settings 24
  Windows services General settings 23
  Windows services Logging settings 23
server administration guides 8
shadow password 19, 35
share points
  creating 42
  defined 29
  for Windows users 18
  managing SMB 41
  naming 42
  planning 30
SMB (Server Message Block) protocol 13
Standalone Windows services 20
status, Windows service 52
strict locking
  described 41
  enabling 42, 43

T

TCP/IP Networking 26

U

user accounts
  changing 33
  defined 29
  deleting 38
  disabling 38
  guest 37
  home settings 36
  locations 31
  PDC 31
  read/write directory 32
user profiles 12, 34
users, disconnecting 53

W

Windows clients
  See also Windows workstations
  cross-platform guidelines 18
  limiting 56
  TCP/IP setup 26
  using file services 25
Windows Computers account
  adding computers to 39
  deleting 40
  editing computer information 40
  moving a computer from 40
  removing computers from 40
Windows services
  Access settings 24, 55
  Advanced settings 24, 57
  assigning server to workgroup 55
  authentication 18
  code page 57
  connected users 53
  connecting by name or address 27
  connecting from Network Neighborhood 26
  disconnecting users 53
  domain browsing 24, 57

General settings 23
graphs 53
guest access 55
limiting connections 56
logs 53, 56
monitoring 52, 53
password validation 18
planning 18
registering with WINS server 58
starting 25, 51
status 52
stopping 51
TCP/IP setup 26
Windows user account settings 34
Windows workstations
adding to Windows Computers account 39
connecting to file service 26, 27
joining PDC 30
removing from Windows Computers account 40
setting up printing 27
WINS (Windows Internet Naming Service)
registering with 58
servers 24
workgroup, changing 55
Workgroup Manager 14
adding to the Windows Computers account 39
Advanced settings 35
Basic settings 33
configuring an SMB share point 43
creating share points 42
creating user accounts 31, 32
deleting a user account 38
disabling a user account 38
editing user accounts 33
Group settings 36
Mail settings 37
managing group accounts 38
Print settings 37
removing from the Windows Computers account 40
setting up a home directory 36
Windows settings 34